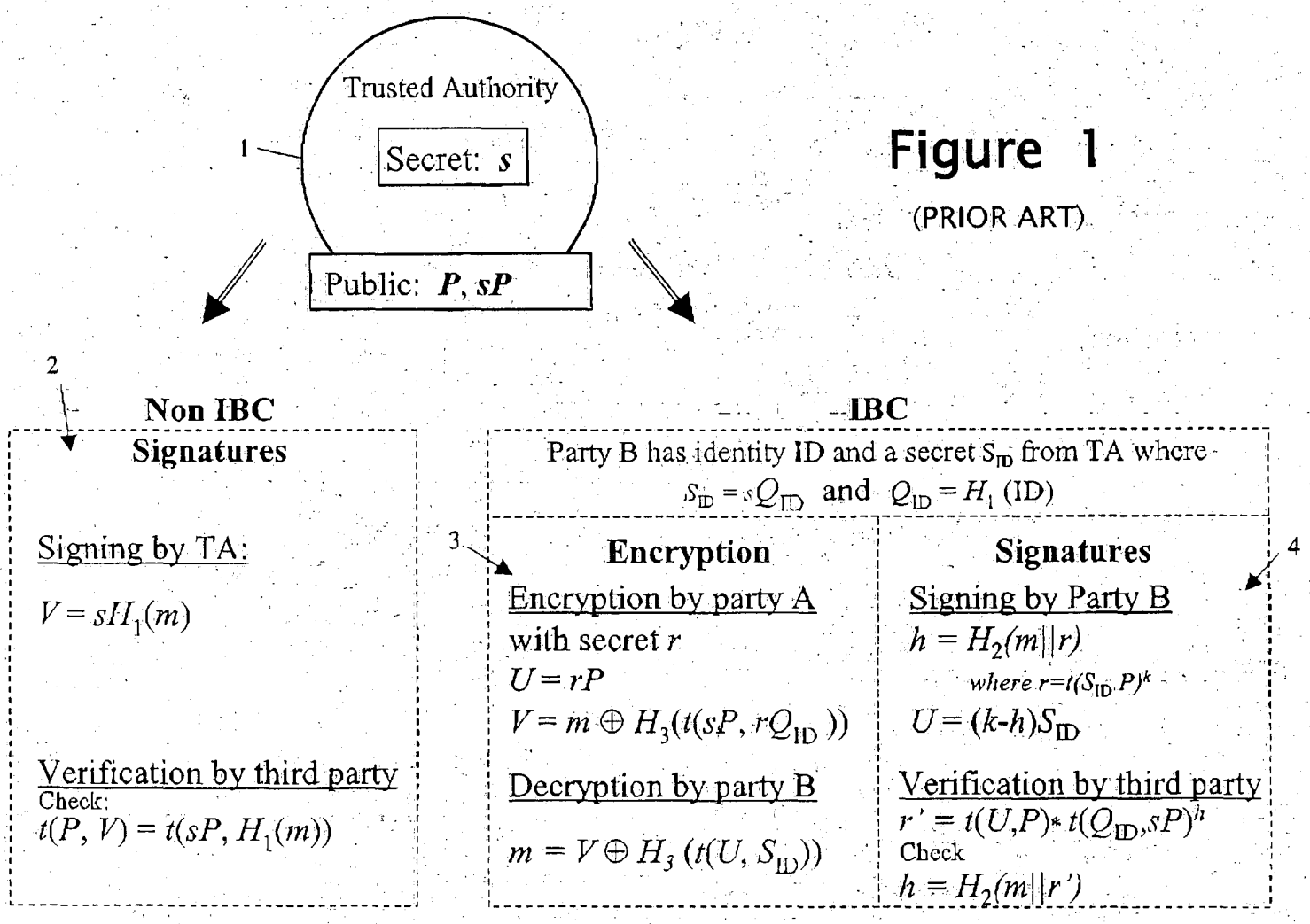

Figure 1

(PRIOR ART)

1/3

EV258281340US

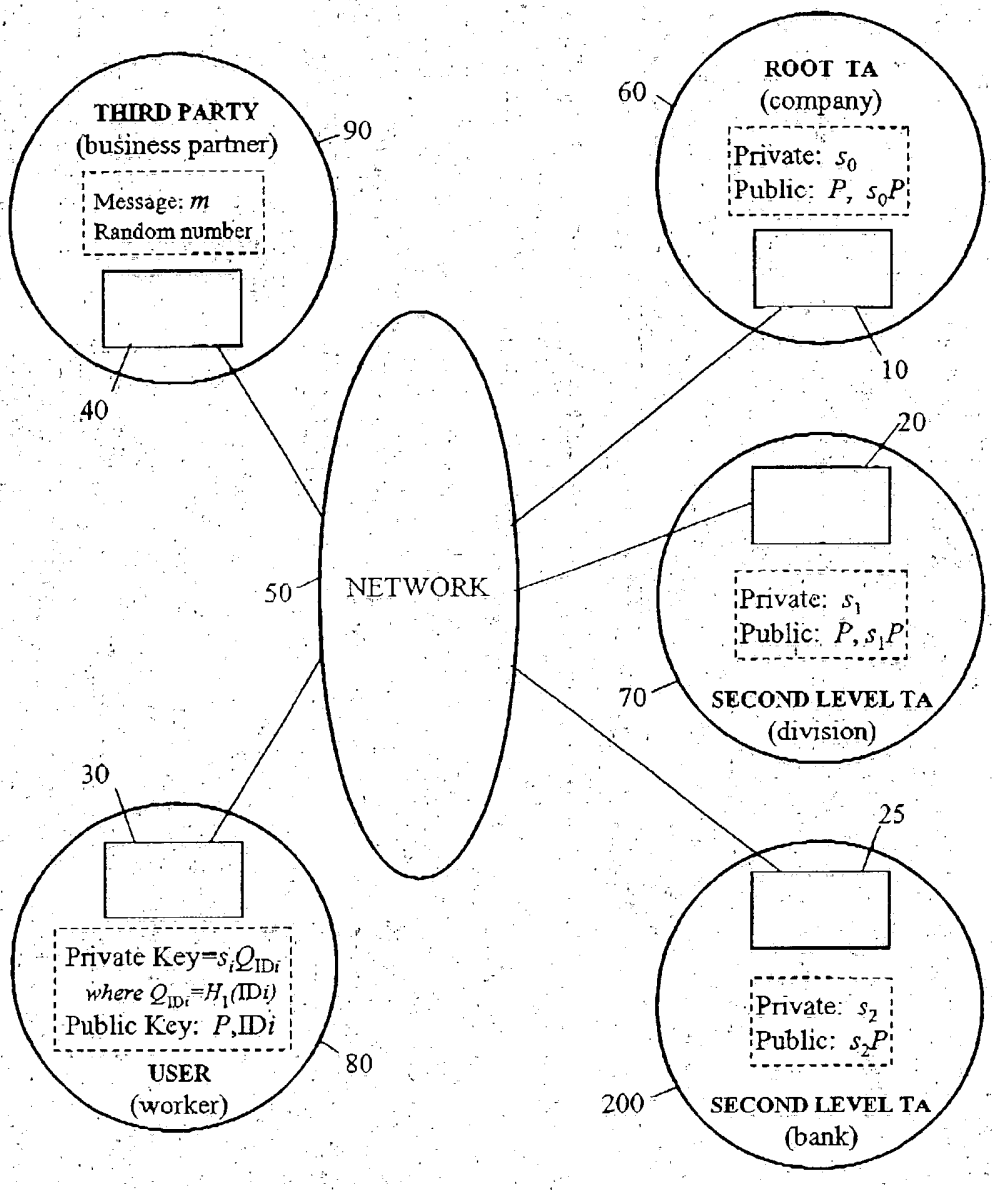
THIRD PARTY
(business partner)
Message: m
Random number
90
40
ROOT TA
(company)
Private: s_0
Public: P, s_0P
60
10
NETWORK
50
20
Private: s_1
Public: P, s_1P
SECOND LEVEL TA
(division)
70
30
Private Key=s_iQ_{IDi}
where $Q_{IDi}=H_1(IDi)$
Public Key: P,IDi
USER
(worker)
80
25
Private: s_2
Public: s_2P
SECOND LEVEL TA
(bank)
200

Figure 2

Embodiment	Key Type	Identity Element	TA Element	Session Element	General Form
First	Encryption "Enc"	Q_{IDi} Public	R_{TAi} Public	r Private	$\prod t(R_{TAi}, rQ_{IDi})$
	Decryption "Dec"	S_{IDi} Private: Q_{IDi} in S_{IDi}	s_i in S_{IDi}	U Public	$t(U, \sum b_i S_i)$
Second	Encryption "gID"	Q_{IDi} Public	P_{pubi} Public	σ Private	$\prod \hat{e}(Q_{IDi}, Ppubi)$
	Decryption "x"	d_{IDi} Private: Q_{IDi} in d_{IDi}	s_i in d_{IDi}	U Public	$\hat{e}(\Sigma d_{IDi}, U)$
Third	Signature (compound)	d_{IDi} Private	P_{pubi} Public	z Private	$h \Sigma d_{IDi} + z \Sigma P_{pubi}$
	Verification (compound)	Q_{IDi} Public	P_{pubi}, U Public	U Public	$\prod \hat{e}(P_{pubi}, hQ_{IDi} + U)$
Fourth	Signature "e"	d_{IDi} Private: Q_{IDi} in d_{IDi}	s_i in d_{IDi}	k Private	$\hat{e}(\Sigma d_{IDi}, P)$
	Verification ""e""	Q_{IDi} Public	P_{pubi} Public	h, S Public	$\prod \hat{e}(Q_{IDi}, P_{pubi})$

Figure 3